Federal Network Security

FNS
Cybersecurity Performance Management

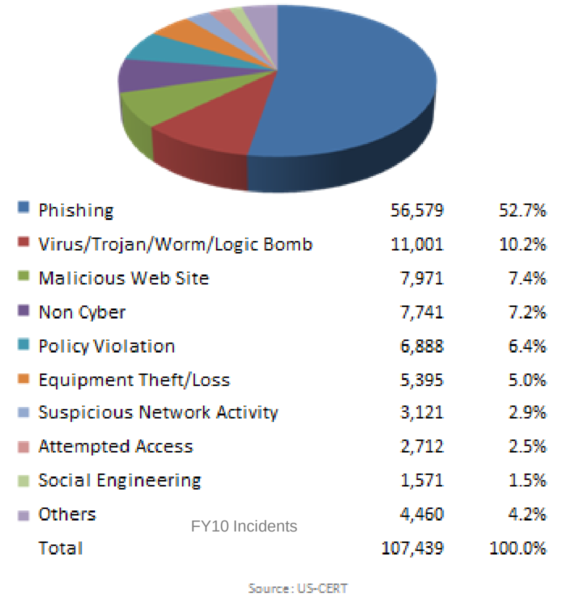
September 13, 2011

Agenda

- Players
  - The Threat
  - The Defenders
- The FISMA Perspective
  - Intent
  - Process
  - Core Capabilities
  - Metrics Approach
- Planning and Driving Progress
  - FY10 Results
  - Action Plans
- FY11 FISMA
  - Monthly Reporting
  - Software Assurance Metrics

Players: The Threat

- Attackers - Nation-States, Criminals, etc…
- Only Need to Find 1 Vulnerability
- Will Exploit Anything
  - People
  - Software
  - Physical Controls
  - Configurations and System Policies
  - Architectural Designs
  - Combinations of the Above



🟦	Phishing	56,579	52.7%
🟥	Virus/Trojan/Worm/Logic Bomb	11,001	10.2%
🟩	Malicious Web Site	7,971	7.4%
🟪	Non Cyber	7,741	7.2%
🟦	Policy Violation	6,888	6.4%
🟧	Equipment Theft/Loss	5,395	5.0%
🟦	Suspicious Network Activity	3,121	2.9%
🟥	Attempted Access	2,712	2.5%
🟩	Social Engineering	1,571	1.5%
🟪	Others	4,460	4.2%
	Total	107,439	100.0%

FY10 Incidents

Source: US-CERT

Players: The Defenders

- Defenders – CIO, CISO, NOC, SOC, …Individual User
- Must Eliminate or Minimize Numerous Potential Vulnerabilities
    - People
    - Software
    - Physical Controls
    - Configurations and System Policies
    - Architectural Design
- Have Limited and/or Dispersed Budgets and Resources
- Support Critical Missions with Complex IT Environments
- Potentially Receive Direction from Various Sources
    - Mandates, Audit Bodies, FISMA, CNCI, etc…
- Don’t Always Have Authority Over All Systems/Infrastructure

FISMA Perspective: Intent

Policies, etc…

Federal Information Security Management Act of 2002

OMB Circular A-130

NIST Special Publications, FIPS

OMB Memos, etc…

Intent

Protect Networks, Systems, and Data:

Proactively, Effectively, and Efficiently Mitigate Threat Vectors

Base Decisions on Risk

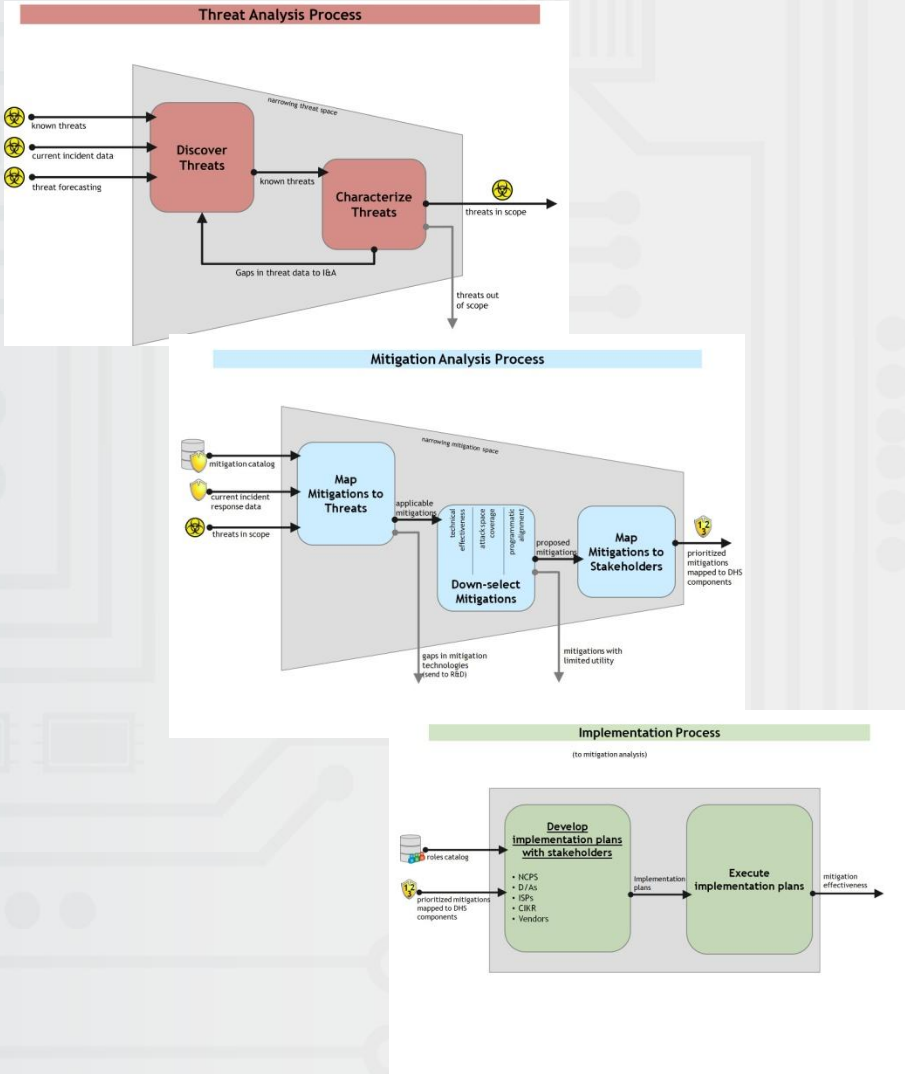
Inform Decisions with Accurate/Timely/Complete Data

FISMA Metrics

FISMA Perspective: Process

- Analyze Incidents/Vectors
- Define Mitigation Options
- Prioritize Mitigations
- Implement Mitigations
- Measure Effectiveness

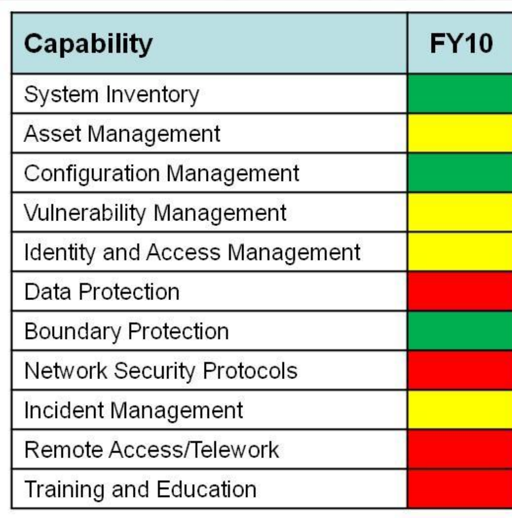
FISMA Capability Framework



FISMA Perspective: Core Capabilities

- FISMA Metrics are Focused on Improving Core Capabilities to Best Reduce Risk – Outcome Focused, Not Compliance!
- Framework Includes:
  - NOC/SOC Capabilities
  - Implementation of Various Capabilities
  - Continuous Monitoring!
- Requires More than Just the Right Metrics
  - Stakeholder engagement/accountability
    - CyberStats/Interviews
    - CISO Advisory Councils
  - Fixing the “Soft Stuff” makes Progress Easier:
    - CFO Engagement
    - IG Relationship
    - Threat Informed Governance

Notional Scorecard



Capability	FY10
System Inventory	🟩
Asset Management	🟨
Configuration Management	🟩
Vulnerability Management	🟨
Identity and Access Management	🟨
Data Protection	🟥
Boundary Protection	🟩
Network Security Protocols	🟥
Incident Management	🟨
Remote Access/Telework	🟥
Training and Education	🟥

3 Levels of Metrics/Maturity

Implementation Levels (Manual Reporting)

Effectiveness/Quality Levels (Partially Automated Reporting)

Impact Levels (Automated Reporting)

FY10 Core Capability Baseline

Capability																									Chg	Avg Totals
Asset Management (1)	71	46	100	91	97	89	53	94	89	72	69	22	71	60	100	100	69	95	84	75	53	98	84	100	A	78.42
Configuration Management (1)	11	0	69	45	48	72	46	61	0	61	48	0	0	54	29	96	66	34	84	53	53	66	64	93	A	48.04
Vulnerability Management	16	6	74	48	61	87	64	88	100	48	32	9	7	50	100	98	63	56	99	75	32	85	64	78	A	60.00
Identity and Access Mgmt	0	0	0	2	0	3	0	0	0	0	1	0	0	0	0	83	90	0	0	0	0	0	0	0	A	7.46
Data Protection	100	78	100	84	2	49	94	100	22	4	91	75	91	100	90	1	43	23	89	98	84	60	100	83	A	69.21
Remote Access – Telework (1)	17	0	100	100	75	0	14	52	0	50	13	56	75	100	0	67	33	100	73	100	100	100	100	100	A	59.38
Remote Access – Telework (4)	67	50	100	100	100	100	71	72	50	100	40	56	25	86	100	67	100	0	63	100	100	100	100	100	A	76.96
Boundary Protection (1)	75	85	81	100	73	94	0	81	75	100	35	95	81	95	80	81	81	95	98	100	93	81	83	81	M*	80.96
Boundary Protection (2)	35	85	48	100	0	29	0	48	100	100	0	65	48	55	95	48	48	100	51	99	93	48	100	48	M*	60.13
Boundary Protection (3)	75	51	0	98	0	42	58	88	5	100	45	5	0	35	0	100	98	0	62	5	48	99	50	49	A	46.38
Incident Management (1)	0	100	0	0	73	61	65	15	67	100	73	100	0	55	95	73	0	95	100	100	95	99	75	98	A	64.13
Incident Management (2)	86	30	85	100	98	95	70	75	93	100	77	90	95	95	95	93	93	97	100	100	95	100	100	98	A	90.00
Training and Education (2)	95	100	100	78	100	100	86	90	100	1	99	100	96	97	98	97	90	94	75	52	97	98	100	99	A	89.25
Training and Education (3)	100	75	2	100	93	96	94	95	82	86	82	75	83	99	89	50	94	64	51	22	96	68	100	100	A	79.00
Network Security Protocols (1)	45	0	0	98	86	68	100	61	0	70	77	62	77	18	88	1	4	56	23	100	96	0	50	100	W	53.33
CIO Score	**1187**	**954**	**1144**	**1645**	**1199**	**1568**	**1279**	**1511**	**1152**	**1454**	**1273**	**1176**	**1200**	**1397**	**1542**	**1423**	**1619**	**1453**	**1521**	**1591**	**1661**	**1781**	**1778**	**1823**		**1430.46**
Percentage Score	51.61	41.48	49.74	71.52	52.13	68.17	55.61	65.70	50.09	63.22	55.35	51.13	52.17	60.74	67.04	61.87	70.39	63.17	66.13	69.17	72.22	77.43	77.30	79.26		62.19

🟩	🟨	🟥
95 and >	50 -94	< 50

Action Plans

(Notional Data)

Capability	FY10	2011 Q4	2012 Q2	2012 Q4
System Inventory	95	98	98	98
Asset Management	25	25	30	35
Configuration Management	60	80	80	85
Vulnerability Management	85	85	85	85
Identity and Access Management	0	20	30	35
Data Protection	45	60	80	80
Boundary Protection	90	90	90	90
Network Security Protocols	55	55	55	60
Incident Management	25	25	40	40
Remote Access/Telework	65	65	75	75
Training and Education	80	90	90	95

NOTE – All projections are subject to financial and internal agency policy constraints.

FY11 Metrics Approach

- Focus CIO Metrics on targeted capability areas that have a direct impact to security
- Represent a logical progression of inquiry from FY10 to help measure agency progress towards capability objectives
- Focus IG community on exploring management & organizational challenges/barriers for capability adoption

FY11 Monthly Reporting Timelines

- Monthly/Quarterly Reporting Guidance Memo
- Monthly Reporting Required
- Due on the 5th of each month, following reporting period
  - (i.e. August Report due Sept 5)
- Monthly Reports only require Auto-Feed Data
- Metrics and Schema (LASR) are Identical to FY10 Annual Auto-Feed Metrics
  - CPEs, CCEs, CVEs
- Changes to Metrics will occur over time

FY11 FISMA: Software Assurance

12.1 Provide the number of information systems, developed in-house or with commercial services, deployed in the past 12 months.

12.1a. Provide the number of information systems above (12.1) that were tested using automated source code testing tools.(Source code testing tools are defined as tools that review source code line by line to detect security vulnerabilities and provide guidance on how to correct problems identified.)

12.1b. Provide the number of the information systems above (12.1a) where the tools generated output compliant with:

12.1b(1). Common Vulnerabilities and Exposures (CVE)
12.1b(2). Common Weakness Enumeration (CWE)
12.1b(3). Common Vulnerability Scoring System (CVSS)
12.1b(4). Open Vulnerability and Assessment Language (OVAL)

2011 Federal Cybersecurity Conference and Workshop

Registration
<http://www.regonline.com/Register/Checkin.aspx?EventID=989639